Quarterly Review

Volume 14 **Issue No. 1** **Spring 2020**

Ohio Association *of* Civil Trial Attorneys

A Quarterly Review of Emerging Trends in Ohio Case Law and Legislative Activity...

Contents

OACTA
Ohio Association of Civil Trial Attorneys
The Source for Defense Success

Compliance Tips for Law Firms and Lawyers To Minimize Cyber-Related Legal Liability

David J. Oberly, Esq.
Blank Rome LLP

While no type of business is immune to hackers today, law firms in particular have found themselves to be especially vulnerable and susceptible to criminal cyber activity, with firms of all sizes experiencing more attempted—and many times successful—cyber attacks from malicious outsiders and data compromise events stemming from firm employees. At the same time, the scope of potential legal liability exposure faced by law firms in connection with data compromise events has also expanded rapidly as well. As such, firms must take proactive measures to shield client data from unauthorized access and acquisition, which can be accomplished through the implementation of several key data security measures as part of an overall cyber risk management program. Executed properly, effective law firm cybersecurity measures can protect law firms not only from experiencing a catastrophic data breach incident, but from substantial potential liability exposure as well.

The Noteworthy Cyber and Security Threat Faced by Law Firms

Cyber attacks on law firms have become so commonplace today that it is no longer a matter of *whether* a firm will fall victim to a cyber-attack, but a question of *when* and *to what extent* a cyber-attack will occur. There are several reasons why law firms are such magnets for cyber attacks.

First, law firms possess a treasure trove of sensitive client data—data which has significant value—rendering them a principal target of cyber attacks aimed at accessing that private firm data, which is then sold on the black market. Second, law firms have money, and lots of it, making them the ideal target for ransomware attacks, where cyber criminals can make easy money by locking down a firm's files until a ransom payment is made.

Third, law firms today are still generally ill-prepared to deal with the sophisticated cyber attacks that are being carried out by cyber criminals today. Broadly speaking, the operation of law firms is still not managed as closely or efficiently as other businesses. Despite the growing threat, many firms have failed to take note and implement the appropriate policies, procedures, and other safeguards that are required to mount an effective defense against today's sophisticated cyber attacks. For the malicious hacker, then, a law firm's computer network may be much easier to penetrate than that of its client.

Increased Scope of Cyber-Related Legal Liability Faced by Law Firms

To further complicate matters, law firms face significantly expanded potential cyber-related legal liability as compared to years past.

First, the threat of legal malpractice claims stemming from data breach incidents or other cybersecurity-related failures is no longer merely theoretical, but now constitutes an actual and significant threat to law firms. While relatively few malpractice claims have been pursued by clients against their attorneys to date, the increasing standards that are rapidly developing regarding the implementation of proper data security safeguards will inevitably lead to an increase in the number of cyber-related legal malpractice claims that are filed as time progresses.

In fact, that trend has already started, first in *Shore v. Johnson & Bell,* No. 16-cv-4363 (N.D. Ill. 2016), a class action lawsuit that was filed against a Chicago law firm for alleged cyber vulnerabilities and failing to protect the security and confidentiality of its thousands of clients

and former clients. Similarly, in *Millard v. Doran,* No. 153262/2016 (Sup. Ct. N.Y. Co. 2016), a legal malpractice action was filed against a New York attorney for allegedly lax data security measures that allowed cyber criminals to send fraudulent instructions to a client during a real estate transaction which, in turn, caused the client to erroneously wire $2 million in funds to the account of the hacker.

While both of these cases were resolved shortly after suit was filed and without an adjudication on the merits, *Shore* and *Millard* provide plaintiffs with a clear blueprint for pursuing legal malpractice claims against law firms and attorneys in the wake of a data security incident involving clients' sensitive or confidential personal information.

Furthermore, in addition to targeted legal malpractice claims, law firms and attorneys are also now vulnerable now to more general negligence claims arising from inadequate cybersecurity measures and data breach incidents. For example, in *Dittman v. UPMC,* 196 A.3d 1036 (Pa. 2018), the Pennsylvania Supreme Court held that employers have an affirmative duty to take reasonable care to safeguard sensitive personal information possessed by the company from cyberattacks. The *Dittman* ruling is a watershed event in cybersecurity and data breach litigation, as the decision establishes new rules of the road for negligence claims asserted in the wake of data breach incident. Importantly, the *Dittman* ruling is applicable well beyond only the employer-employee relationship, and likely applies with equal force in other contexts, including attorney-client relationships.

In addition, law firms and lawyers now also face liability in connection with new consumer privacy laws that are starting to be enacted across the country. For example, the California Consumer Privacy Act of 2018 ("CCPA")—which went into effect at the start of 2020—requires companies, including law firms, to comply with a range of requirements and limitations regarding the collection, use, and sharing of personal data of California residents. In addition, the CCPA provides consumers—including law firm clients—a private right of action to pursue class action litigation in connection with certain data breach events, with available statutory damages of $100 to $750 per incident. Other state legislatures across the nation have made a concerted effort to enact similar "CCPA copycat" laws of their own, and it is highly likely that other states will be successful in putting in place their own versions of the CCPA in the coming months and years.

Compliance Steps

Combined, law firms and lawyers face noteworthy potential legal liability in connection with data breaches and other types of data compromise events. Fortunately, there are several proactive measures that firms and attorneys can take to minimize the risk of cyber-related legal liability:

- **Cybersecurity/Data Security Policies & Procedures:** As a starting point, firms should develop and implement a stringent set of cybersecurity and data privacy policies and procedures addressing the use of technology by firm personnel. These policies should define expectations for employees, as well as anyone with access to firm data, regarding issues such as the use of personal email and devices, file-sharing programs, the copying of data to personal devices, and use of firm systems from remote locations. Important policies to have to reduce the risk of cyber-related legal liability include acceptable use, Internet use, mobile device and tablet, bring-your-own device ("BYOD"), and password policies.

- **Firm Personnel Education & Training:** Education and training is a second vital ingredient to any effective firm cybersecurity risk management program, as many data compromise incidents are either directly or indirectly caused by human error or carelessness. In particular, firm employees should be made aware of the vital importance of safeguarding firm data and the key role that firm personnel play in ensuring the security of the organization's networks and systems. Furthermore, firms should also educate personnel on effective cybersecurity practices, such as being suspicious of potential phishing emails, and the ability to spot social engineering schemes, which have become a go-to tactic for hackers attempting to infiltrate firm networks through human vulnerabilities.

- **Maintaining a Security-First Firm Culture:** Beyond mere education and training, firms should also strive to promote a cybersecurity-first culture throughout their organizations. This can be done in a variety of ways. Set achievable, firm-wide security goals. Connect the security of the firm to the personal privacy of employees

CONTINUED

themselves. Communicate clear rules and requirements regarding the use of technology at work. Educate employees about the business benefits, and potential severe negative consequences, that employees' cyber habits have on the firm. Post reminders around the office relating to cyber-attack prevention measures. Combined, with the proper amount of time and effort, firms can develop a mindset and culture throughout the organization that maximizes employees' commitment to making cybersecurity a top priority in their day-to-day activities, which in turn can play a significant role in preventing cyber attacks from wreaking havoc on a firm's systems and finances.

- **Vendor Management:** In addition to assessing the security of their own systems, firms also need to assess the security of their vendors as well, as law firms' support vendors can often serve as the weakest link in a firm's security chain due to inadequate security controls and the entry portal these entities possess to firm systems. As part of the vendor selection process, firms should conduct thorough due diligence and evaluate the vendor's data security practices and procedures. Once a vendor is retained, firms should ensure that vendor access to firm data, as well as the vendor's ability to make changes on the firm's system, is limited to the greatest extent possible. In addition, firms should also develop necessary contractual security requirements for all vendors that maintain access to the firm's client information or systems.

- **Cyber Insurance:** Finally, firms should obtain cyber-specific insurance coverage (if they have not already done so) to mitigate the risk of expenses and losses resulting from a data breach incident. Law firms cannot assume that their general firm insurance policies will cover all losses stemming from a cyber attack, as many firms have discovered the hard way that their professional errors and omissions insurance, general liability insurance, and property insurance do not cover all of the costs associated with a cyber attack. Cyber insurance coverage, on the other hand, is specifically designed to cover losses stemming from a data breach, both in terms of response costs for things like providing notice of a breach, as well as damages and expenses arising out of lawsuits stemming from the breach. Importantly, in addition to covering direct losses stemming from a breach, cyber-risk policies will also cover indirect costs and expenses associated with the breach, such as public relations firm costs, legal fees, and credit monitoring services fees.

Conclusion

Due to the massive volume of sensitive, highly valuable client information that is collected and maintained, as well as the noteworthy amount of revenue generated, law firms are particularly prime targets for cyber attacks. Recently, malicious hackers have stepped up the frequency and sophistication of their attacks against law firms large and small, with firms now facing far greater security threats than ever before. Cyber attacks on law firms are only likely to escalate and intensify moving forward, as cyber criminals develop new techniques to infiltrate firm systems and networks in more advanced ways. At the same time, firms and attorneys also face significantly expanded liability in connection with cybersecurity and data security incidents as well.

As such, it is critical for law firms to implement effective measures to properly safeguard their networks and systems, as well as the data they possess. Through the implementation of the cybersecurity practices and safeguards discussed above—as part of a comprehensive cybersecurity risk management program—law firms can take proactive precautionary measures to effectively minimize the risk of falling victim to a cyber attack and, more importantly, avoid being on the receiving end of a potentially catastrophic cyber-related lawsuit arising from cybersecurity and data security shortcomings.

David J. Oberly, Esq, is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy and Privacy Class Action Defense groups. David's practice encompasses both counseling and advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters, as well as representing clients in the defense of privacy and biometric privacy class action litigation. He can be reached at doberly@blankrome.com. You can also follow David on Twitter at @DavidJOberly.